Policy Privacy and Security
Draft Transcript
January 22, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you very much, and welcome to the privacy and security policy workgroup. This meeting will close at noon, and a few minutes before noon, there will be opportunity for the public to make comments. I'll turn it over now to Deven McGraw, the chair.

Deven McGraw - Center for Democracy & Technology – Director
Great. Thank you. Those of us on the committee heard the sort of *Rocky* like theme before the public came in, which….

M
Yes. Can we get that every time?

W
Aren't you at the Philadelphia Library?

Deven McGraw - Center for Democracy & Technology – Director
No, actually I'm not. I'm north of Philadelphia, but at any rate, I think that was an interesting way to start our call today.

M
I think before Paul Tang speaks it should happen, any time before he speaks.

Deven McGraw - Center for Democracy & Technology – Director
Da-ta-da-da.

M
Yes, theme music from *Peewee's Playhouse*. I think that fits me.

Deven McGraw - Center for Democracy & Technology – Director
Okay. All right. We do have some things to get done today. Just an overview of the agenda, we're going to spend most of the time talking about what we might recommend to the policy committee with respect to some comments on the meaningful use and standard certification criteria rules. And then what I hope to do sort of towards the end of the meeting, unless we're running out of time, although I may even start this conversation even if we're sort of not done with our recommendations because we do have one more call scheduled between now and the next policy committee meeting, which is in mid February, so this is not our last bite at the apple with respect to recommendations, but I wanted to get us as far as we could.

But what I hope to be able to do with a little bit of time on this call since the issue of patient preference, patient choice, sometimes referred to as consent, sometimes referred to as opt in, opt out, is really weighing heavy on a lot of people's minds. I want to start talking about – I want to start building a work plan for how we're going to tackle this. And maybe get some feedback, not to discuss substance or start talking necessarily about what our recommendations might look like in this space, but more about sort of what information do we think we're going to need in order to help us answer this question, whether it's vendor capacity, whether it’s what’s going on out there now with respect to states and health information organizations on this issue, etc. I just want to start teeing that up. I know everyone – again, I know it’s a concern of a lot of people, and we’re pulling together a work plan for that, and I’d like to begin to start pulling some feedback from you all on that during this call, and then we’ll close with public comment.

Peter Basch – MedStar Health – Medical Director
Deven, it’s Peter. Before we get started on that because I think that could take the entire meeting, I had a question on page two of the agenda, the second paragraph where it says towards the end, “Clarify the language and the care coordination section of the policy committee’s MU matrix regarding sharing data with patient authorized entities.”

Deven McGraw - Center for Democracy & Technology – Director
That’s right.

Peter Basch – MedStar Health – Medical Director
Is that something we are doing?

Deven McGraw - Center for Democracy & Technology – Director
No. This is actually more a note to me, but since I gave you so much annotation on the agenda, it ended up being kept in there. This was – we had – I can’t remember, Peter, if you were on our last call, but there was some discussion about whether that – what that language meant and whether that was some sort of opening that we should try to use to put some recommendations to the policy committee with respect to patient consent and maybe when it should be obtained, etc. And so that’s just, again, since we were, and that was sort of towards the end of the call, and I wanted to make sure that everyone was clear that, with respect to that particular piece of the matrix, the reason why that language is there is because it’s a data sharing section of the meaningful use matrix that the policy committee came up, and it’s….

Peter Basch – MedStar Health – Medical Director
You’re talking about the July meeting?

Deven McGraw - Center for Democracy & Technology – Director
Yes. Yes, and it was intended to refer to the sharing of data, not necessarily among providers, but also with entities that the patient authorizes, and so it deals both with the sort of new requirements under the stimulus legislation, ARRA, that when patients have a right to an electronic copy, they can get it sent to someone or another entity like a PHR vendor. And then also, I think it also encompasses those, when patient authorization is currently required by law and needs to be obtained, obviously if a physician is sharing data, that’s an patient authorized entity. But it was not, since I helped develop that matrix, it wasn’t necessarily intended to mean anything broader than sort of where current law is with respect to choices that patients have in sharing the data.

Peter Basch – MedStar Health – Medical Director
Right. I just wanted to be sure that looking at this from a broader perspective, as opposed to just the privacy and security perspective that this workgroup is doing, that my literal read of your notes to self, and I didn’t really understand it was a note to self, we’re not redefining what care coordination is.

Deven McGraw - Center for Democracy & Technology – Director
No.

Peter Basch – MedStar Health – Medical Director

Yes, because the way it reads was the language was intended to refer to, so I was going to make a point it could include sharing, but we're not rewriting….

Deven McGraw - Center for Democracy & Technology – Director
Right. All right. But now that you know my intent … feel better?

Peter Basch – MedStar Health – Medical Director
Move on.

Deven McGraw - Center for Democracy & Technology – Director
My apologies for that. It was a source of discussion on the last call, and I wanted to make sure everyone was clear, certainly, about what was intended vis-à-vis the privacy and security aspects. Okay. So going back to page one of the agenda is, again, the Health IT Policy Committee is going to be submitting formal comments, which are likely to come in the form of recommendations similar to what we had done with the meaningful use matrix to begin with to both the National Coordinator, as well as CMS, on the meaningful use proposed rule and the standards and technology criteria interim final rule. Those comments will really need to be finalized by the policy committee at its February 17th meeting in order to insure that it can be duly submitted within the comment period on those rules.

And so, subsequently, the policy committee has tasked each of its workgroups to submit comments or recommendations for any of the proposed or interim final rules that fall within our charge. So our goal is to come up with those comments or recommendations and to get a good chunk of that, I think, done on this call to focus on the privacy and security aspects of those rules because that is our charge. And then, again, whatever we're not able to complete in this meeting, we'll pick up on our next call. Actually, what we'll also do on our next call is look at the articulation of those recommendations, so people are comfortable that we have sort of captured it appropriately in the language. Does everybody understand that?

M
Yes.

M
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Okay. Terrific. All right. So what I've proposed to do here is to start with the meaningful use proposed rule, which covers stage one of meaningful use criteria, which is going to be 2011 to 2012 for folks, for providers and hospitals who are early adopters, who want the financial incentives in the early years. Stage one ties to those early years of adoption. And the sole objective in the meaningful use proposed rule on privacy and security is protecting health information through the implementation of appropriate technical capabilities, and the sole measure for that, as we started to discuss last time, is conducting or reviewing a security risk analysis, which is already required under the HIPAA security rule, and then implementing security updates, as necessary, and then the proof of that is attestation by the eligible provider or the hospital.

What was rejected was a policy committee suggestion to make HIPAA compliance an expressed meaningful use objective and to deem providers who are under formal investigation, not complaint, for a HIPAA rule violation to be ineligible for any financial incentives until that gets resolved. As I think it was Dave Wanser on our last call pointed out, there was also no specific objective or measure regarding increased transparency to patients regarding uses of data, even though it was part of the policy committee matrix. But, admittedly, the committee matrix didn’t really specify any details at all on this issue in terms of sort of what would be a more clear objective in that regard. How would physicians or hospitals demonstrate that? And probably in part because, in fact, if you’re complying with HIPAA, you have to at least provide a notice to patients about what HIPAA allows with respect to access use or disclosure of data. Of course, folks could reasonably disagree on whether that’s terribly transparent to folks in its current form, but it certainly is a requirement.

Then, in addition to these departures from what the policy committee had recommended, there may be some other concerns to possibly address, and some of these came up on our last call: lack of knowledge about how to do security assessments, what is meant by this requirement to implement “updates as necessary”, and no clear connection of the meaningful use requirements or the requirement to implement security updates to in fact the new security technology functionality requirements that are required to be in the technology that is purchased using the financial incentive under the legislation.

It teed up a couple of ideas for discussion, and I divided them into two sections. The first being looking at what’s in the existing meaningful use rule, what do we want to say to improve that in any way, if anything. And then the second topic area is to the extent that there were criteria that were put on the table by the policy committee that were rejected, or are there some that are new that we might propose? Then I had some suggestions written out there just to guide our discussion today. I mean, we’re certainly not wedded to these at all, but I wanted to lay some things on the table for us to discuss so that we could be a little bit more focused, given the size of our group.

I think we should start with what we might recommend with respect to existing meaningful use criteria, and this is on the need to do a security assessment. As you’ll see, it’s suggested that ONC provide education to eligible providers and hospitals on the components of a good security risk assessment. Perhaps it should be a joint effort with expertise across the board. Someone actually mentioned to me yesterday that in fact HL-7 is developing some guidance on this, which could be helpful. And these materials could then be disseminated and shared through sort of the usual places where it exists today, guidance on the security rule that is on CMS, as well as the Office of Civil Rights Web site. It could be on ONC’s Web site as well, as well as through regional extension centers, state health IT offices, regional program offices, and then I put specialty societies on there, but I have no idea whether that makes any sense.

Then I suggested that maybe we need to make more clear that the need to attest to the security assessment is for all years of participation in the meaningful use program since the security rule requirement to do that risk assessment is annual, and the right is I just wanted to check for the other lawyers on the phone on that one. And then the attestation should be both to the performance of the risk assessment, as well as the implementation of any updates that are deemed to be necessary. I’m not suggesting that providers should have to disclose what these are, although we can talk about that. But they should keep documentation in the event of an audit. Laying all of that out, I would like to open it up for a discussion about what you think of these.

John Blair – Hudson Valley HIE – President & CEO
Yes. Deven, this is John Blair. Can I make a couple comments?

Deven McGraw - Center for Democracy & Technology – Director
Of course.

John Blair – Hudson Valley HIE – President & CEO

Yes, so two things. One, how are we going to deal with the different capabilities from a solo practitioner up to an IDN on this kind of communication education? The second is, have you thought about the EHR vendors, which will have, you know, they'll be dealing with each of these practices, and having to deal with meaningful use, so what about some type of obligation for them or part of what they're offering in terms of helping these practices get to meaningful use, adding that? At least that's another potential avenue to get that information and to help the practices.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Deven, this is….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John.

Deven McGraw - Center for Democracy & Technology – Director
Go ahead, John, and then I think that was Dixie.

Joyce DuBow – AARP Public Policy Institute – Associate Director
No, it was Joyce.

Deven McGraw - Center for Democracy & Technology – Director
Joyce, okay.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Thank you for confusing our accents.

Deven McGraw - Center for Democracy & Technology – Director
I'm sorry. I just heard a little voice. Go ahead, John, and then Joyce.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes. I had a couple comments. The first being is that if you really look – doing a security risk analysis, to me, is only part of the bigger picture, and if you really wanted to try to identify an outcome, it's clearly attestation that you fully comply with the HIPAA privacy and security rules, at least as they relate to use of electronic systems. But above and beyond that, I think that if you're looking for concrete measures in which to try to judge against, one of the things that I have asked for, and I think does make sense here is that since audits are supposed to be forthcoming with respect to HIPAA compliance through the Feds, to me typically when there is an audit, there should be an audit program. And audit programs typically very clearly spell out what the expectations are in terms of not just the audit itself, but in terms of what is acceptable and what's not acceptable.

I think what would be helpful to me, and again, I have asked for this on a number of occasions is, is what is the government's audit program if it comes in and audits covered entities for compliance with HIPAA? If you could take that audit program and identify those components that really relate to health IT, then I think you could point to very discrete measures that would be in expectations. And so, again, I think that that might be a way to address the measures component here.

Deven McGraw - Center for Democracy & Technology – Director
Okay. Joyce, and then we'll open it up for more reaction.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Well, I think these are actually more in the form of questions, just to help me understand this.

Deven McGraw - Center for Democracy & Technology – Director
Sure.

Joyce DuBow – AARP Public Policy Institute – Associate Director
First is that under your topics of discussion, I think that it makes good sense to provide the education for people to better understand how to do the security assessments, but it's not clear to me what the relationship is between making a suggestion that there be education and the implications for the NPRM itself. In other words, I think it's a nice thing to have, but I don't see how it strengths the – I don't see how it responds to the concerns we have about the paucity of specificity in the regulation itself in the proposed reg, and so that's a question. It's not an assertion.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Joyce DuBow – AARP Public Policy Institute – Associate Director
The second question is whether there are important implications for their failure to acknowledge that the requirement for a security risk analysis is already part of HIPAA.

Deven McGraw - Center for Democracy & Technology – Director
They did acknowledge that.

Joyce DuBow – AARP Public Policy Institute – Associate Director
It was my understanding that they – oh, so it's there already?

Deven McGraw - Center for Democracy & Technology – Director
Yes. Well, they know that. They just didn't – what they did not do was to take the sort of broader, you must comply with HIPAA as sort of part of meaningful use suggestion that the policy committee put forward. Instead they picked out the security risk assessment that has to be done under the HIPAA security rule and acknowledge that that was part of the security rule.

Joyce DuBow – AARP Public Policy Institute – Associate Director
To clarify my question then, I mean, if we know it exists, then is there any material, legal reason to be overly concerned about it? You know, I'm not seeing some emphasis in there in the meaningful use stuff. In other words, is this a serious concern that we need to address, is really my question, or is it going to be handled because it's already covered by HIPAA?

Deven McGraw - Center for Democracy & Technology – Director
I guess I'm confused. Are you speaking to the question of whether there ought to be a sort of HIPAA compliance piece overall to the meaningful use rule?

Joyce DuBow – AARP Public Policy Institute – Associate Director
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Can we hold the topic, the conversation on that because that's in the sort of expressly rejected category, and should we bring it back in? I mean, it's related, of course, to this discussion since the security rule piece is in there.

Joyce DuBow – AARP Public Policy Institute – Associate Director
That's fine.

Deven McGraw - Center for Democracy & Technology – Director
Okay. Let me say a couple of things about certainly requiring education is good. It doesn't necessarily increase the specificity of the rule, but I think a lot of us are worried what providers and particularly the non-institutional providers are going to do with being told, being reminded, number one, that they're supposed to do this under the security rule, and now making it part of an attestation of meaningful use, and that they ought to have readily available education materials that I think more ideally would be tailored to the sort of type of practice that they have and size because it may be different, institution versus provider, you know, versus sort of small provider, which sort of gets to John's question.

I don't think we're talking about one size fits all. The security rule is not one size fits all. There's a fair degree of flexibility in there. The idea is you're supposed to do the risk assessment commensurate with the type of system that you've got and what the risks might be. But again, we're asking for physicians to do this essentially and notwithstanding what they may have been required to do under HIPAA. For many of them, it's the first time. And for many of them, it's the first time that they have to do so in the context of adopting technology, so it's very different versus the paper record.

Again, I think that the audit program compliance, you know, to the extent that that is developed and disseminated, that could provide sort of some more kind of hooks for specificity with respect to what needs to be implemented, etc., but we don't have that that I know of, and so we're stuck with what we've got. But that doesn't mean we couldn't have a recommendation that something like that, that if that be developed and that something like that could lead to an ability to be more precise about what's expected.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Deven, this is John Houston again, if I might expand upon my comment just a tiny bit. Being responsible for information security and privacy at a large health system, this is something that I know other people that are in my position are also very interested in. When there's a fear of an audit, you always like to know what you're going to be audited against. So this actually serves two ends. One, it provides some type of measure that people can look to and say, okay, if I look at this audit program, and I look at my – do this assessment or analysis, I should say, what am I going to get measured upon and make sure that those are aligned, and that helps from a meaningful use perspective.

But also, people doing security always want to sort of understand what are the rules, and what am I going to get measured against generally, so forcing that audit program to actually be published, I think, serves, again, not just the meaningful use aspect of it, but it allows people that really want to, in good faith, comply with HIPAA, gives them the ability to do their own assessments in a manner that they would then feel comfortable if the government walks in the door and wants to do an audit. You know, you and I saw that one survey where one f the questions was, do you feel you're compliant with HIPAA? And the answer is, people say yes, but then are they comfortable if the government were to come in and do an audit? The answer is sort of no, or at least not everybody is comfortable with that because they don't know what the audit is going to entail.

Deven McGraw - Center for Democracy & Technology – Director
Right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think this serves two ends here, and I think it would be a good way to approach this.

Peter Basch – MedStar Health – Medical Director
Yes. I would agree.

Deven McGraw - Center for Democracy & Technology – Director
Is this Peter?

Peter Basch – MedStar Health – Medical Director
Yes, it's Peter. I'm sorry.

Deven McGraw - Center for Democracy & Technology – Director
Thanks. That's okay.

Peter Basch – MedStar Health – Medical Director
That one of the problems working in a health system, but also functioning in a clinical environment, a small office, I would say that there's still massive confusion primarily among physicians in large offices about what HIPAA actually requires and what it doesn't, and we're still seeing the aftermath of, I think, poor training and public awareness, as well as, and I apologize if I'm insulting anyone here who was involved in this campaign, but a consultant campaign to, at least in the opinion of some, make HIPAA appear more complex and more onerous than it actually was. I think, if this is an opportunity to come forward on a positive foot of laying out clearly what providers in each setting of care need to do, then let's take it and let's be clear about it, and let's let these rules be known because I also look at each of the metrics for meaningful use as an opportunity, not just to create, I'll use this word again, reasonable hurdle for providers to jump through to get their meaningful use benefits, but also a potential barrier to people considering adopting health IT.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Peter Basch – MedStar Health – Medical Director
So we want this to be done in such a way that it actually may even attract some people to, oh, I get this. This makes sense to me, and now I know what I need to do to comply with it.

Rachel Block – New York eHealth Collaborative – Executive Director
Deven, it's Rachel. I just wanted to let you know, I did join. I apologize for being delayed.

Deven McGraw - Center for Democracy & Technology – Director
No, that's okay. Great. Good to have you, Rachel.

Paul Egerman – eScription – CEO
Deven, this is Paul. Actually, they had me on for 20 minutes as a member of the public before I realized it.

Deven McGraw - Center for Democracy & Technology – Director
Okay. I'm sorry, Paul Egerman. Good to have you on.

Paul Egerman – eScription – CEO
I am here.

Deven McGraw - Center for Democracy & Technology – Director

We have a lot of Paul's, so we're going to have to be careful with that too. Thank you.

M
This is…. I'm sorry. My sense of this, and I certainly agree with what everybody said about transparency, and I think we also might benefit from articulating intended outcomes because compliance with the regulations is not necessarily the intended outcome. The intended outcome is really that you're doing due diligence around incursions or breaches of your systems.

Deven McGraw - Center for Democracy & Technology – Director
Right.

M
And so to the extent that we articulate the outcome, and then the criteria against which those outcomes will be achieved, I think we help people. A question from my end is whether or not the regulations is the best place for those criteria given the effort that it requires to change regulations, and would we need those audit criteria to be more flexible and time sensitive than regulations might allow.

Deven McGraw - Center for Democracy & Technology – Director
Well, I mean, I think here's the reality is, I'm wondering whether we'd have to sort of frame a desire for audit program compliance guidelines as something that is really the responsibility of the regulators to do and, quite frankly, is not likely to be done necessarily in time for us to have sort of more specific criteria here. I think it's more phrased in terms of that this is something that ought to happen in the coming years. Therefore, in whatever educational material is available in 2011 for those early adopters ought to be disseminated, and providers ought to understand sort of, to the best that they can, what they need to do to comply. But ideally there ought to be sort of more specific guidance that gets to what folks would be audited against by authorities so that expectations are a lot more clear down the road.

M
Yes.

Deven McGraw - Center for Democracy & Technology – Director
So I don't see us framing this in terms of we need to have X before we can do any of this because I think that creates an impossibility giving timing and the fact that we just don't have what might be ideal in this space.

Paul Egerman – eScription – CEO
In this whole discussion of audit, I always think about the third party impact. It would seem to me, we should be encouraging ONC and CMS, not just through education, but to work with accreditation organizations and encourage auditing firms to perform this function because a better response than self-attestation, in my opinion, would be if a hospital were to say, well, here's my JAYCO security audit stamp because that's sort of like, to me, that's the way to do that, or for a medical group to say, you know, Deloitte performed an audit. And I almost wonder if we could suggest changing the NPRM to say you could do self-attestation and, as part of the self-attestation, you should say whether or not an accrediting organization or an auditing firm has reviewed this process. Sort of leave open the idea that that would be a better way to go forward in the future.

Peter Basch – MedStar Health – Medical Director
This is Peter.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

How do you think that plays out? I agree with that, but I always am concerned about the small practices.

W
Right.

Peter Basch – MedStar Health – Medical Director
Yes, let me concur. Was that John?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes, that's me.

Peter Basch – MedStar Health – Medical Director
Yes. It's Peter. I would concur because, again, I'm looking back to the debacle that was HIPAA implementation for small practices in terms of fear and loathing as opposed to what many of us hope for, which was understanding that this is and should be part of standard medical practice. The notion that one would have to have security audits on an annual basis by a consulting firm may make this transition to electronic systems not, you know, could make them unaffordable, at least perceive them to be unaffordable, or something out of the reach of small groups.

Paul Egerman – eScription – CEO
Yes. I'm not suggesting, first of all, that we do that in stage on.

W
Well, but you also….

Paul Egerman – eScription – CEO
If I could just say….

W
Sure.

Paul Egerman – eScription – CEO
But what we could do to be responsive to the comments is you could say this concept of an accreditation organization or an auditing organization would apply to hospitals, or it might apply to group practices of 50 or more physicians.

Peter Basch – MedStar Health – Medical Director
Yes, well, I think the spirit of it should go to everybody. I just think we need to be careful about how we craft this.

Paul Egerman – eScription – CEO
Yes, well, maybe there's a way to do it.

Peter Basch – MedStar Health – Medical Director
I go back again to the vendors. If the vendors start to understand, because they implement these, and they train practices, and they need to be training on some of the security aspect of this. It's their system. So if they start to understand there's some responsibility there, and certainly that's part of meaningful use, you do have another avenue. I think the spirit of what was said is right. I'm just saying, let's make sure that we're careful about all concerned.

Deven McGraw - Center for Democracy & Technology – Director
Right, and the other thing to keep in mind, and again, this is Deven, is that certainly under the security rule today, you have an option of pulling an outside entity in to do this for you instead of trying to rely on it yourself.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
By the way, a lot of large organizations and mid-sized organizations, hospitals, will have internal audit staff themselves, and they very well may be incredibly competent at taking, if they had an audit plan, and executing on it, and then doing a certification.

Deven McGraw - Center for Democracy & Technology – Director
Right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
So I think it should be a matter – this should be a preference rather than a requirement in terms of outside audit. Some people may decide that their board feels strongly enough that they do pull in an outside audit firm to be able to provide this audit.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
Basically there are two parts to what I'm saying. The first part is I'm suggesting the NPRM should simply have like a very – for stage one, it should say you should be self-attestation, or should be an indication that a third party audit or an accreditation organization has reviewed this. So it's just sort of a gentle…. It's an option.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
But then also that we should have some recommendation for process, so as we move through stages two and three that ONC put some effort into these auditing firms and accreditation organizations in addition to the other things we talked about in terms of the extension centers. It's not an instead of, but in addition, as a vehicle to move this forward.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dave Wanser – NDIIC – Executive Director
But this is Dave, and I think, again, the upstream issue is clarity and expectation.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dave Wanser – NDIIC – Executive Director
That there's not wide, wide variation around what people are interpreting.

Paul Egerman – eScription – CEO
That's correct.

Dave Wanser – NDIIC – Executive Director
That verification of what the expectations are, being something that RECs can push out as part of their work with small practices is a preventative approach that we should emphasize.

Deven McGraw - Center for Democracy & Technology – Director
Agree.

Peter Basch – MedStar Health – Medical Director
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Does anybody else have any comments on ways to strengthen the existing rule beyond what we've talked about, or does anybody have any objection to any of the other bullets that were under there? Again, we'll augment them based on the discussion that we've had today.

Paul Egerman – eScription – CEO
Are we also going to talk about the security update phase?

Deven McGraw - Center for Democracy & Technology – Director
Yes. Well, go right ahead.

Paul Egerman – eScription – CEO
Well, I mean, that was also a part of what it had said in the NPRM that I thought was weak because I didn't know what it meant.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
I thought I knew what it meant, and so that somebody is going to tell me what I thought it meant is wrong, but I thought it was talking about updates that various vendors have from time-to-time to plugs because of security holes in your software. Is that what that means? What did people think that meant, security updates?

Peter Basch – MedStar Health – Medical Director
That's what I thought it meant.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's what I thought it meant.

Deven McGraw - Center for Democracy & Technology – Director
That's so interesting. That is not what I thought it meant at all because it's meaningful use, not necessarily the technology certification. And so I thought that it meant, if you, in the process of your audit, come up with a security gap, i.e., oh, we don't have, you know, password protection for simple logons for these computers, then you implement it. You basically fix the flaws that you uncover in your assessment.

Peter Basch – MedStar Health – Medical Director

Yes, I think the problem is that for those who work with technology frequently, we tend to think about the term update differently.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Peter, I think that what Deven is saying is right.

Peter Basch – MedStar Health – Medical Director
I don't disagree.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But I think the update is in addition to that.

Peter Basch – MedStar Health – Medical Director
Sure, and that's fine. I think that needs further clarification.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Yes, good point. It never even occurred to me that people might read that and think, oh, you know, it's just the version 2.1.

Peter Basch – MedStar Health – Medical Director
You've got to put your geek face on. That's all.

Paul Egerman – eScription – CEO
Deven, when I read it, I really didn't know what it meant, so I took a guess that's what it meant. You may be completely right, but my suggestion, I think, is also an important thing.

Deven McGraw - Center for Democracy & Technology – Director
Well, I think, let's clarify then.

Paul Egerman – eScription – CEO
I'd like to clarify it, but I would also like them, as part of the clarification to do both, to do what you're saying and also to do what I'm saying.

Deven McGraw - Center for Democracy & Technology – Director
Right. Of course.

Peter Basch – MedStar Health – Medical Director
Right. I think it's an assessment and then acting upon the findings, and then also the update. The thing that I question is if it's the updates, as we're interpreting it here, how do you verify that? That gets really tough.

Deven McGraw - Center for Democracy & Technology – Director
Well, I mean, how do you verify anything on meaningful use? It's all, you know, at least in these early phases, it's attestation, but it's attestation under penalty if you are audited by CMS and found to be wrong.

Peter Basch – MedStar Health – Medical Director
But how do you do attestation of updates?

Deven McGraw - Center for Democracy & Technology – Director
I did them.

Peter Basch – MedStar Health – Medical Director
Every six months, you send in an attestation?

Deven McGraw - Center for Democracy & Technology – Director
No, you say that you did them.

Paul Egerman – eScription – CEO
Yes, I actually know how to do that part.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
I mean, for software updates, there are ways to do this. For large organizations, they could still be part of the accreditation or audit process. Normally the large organizations are audited, and the auditor or the accreditation organization can check on it. For small organizations, for small physician offices, two or three person offices, there are software solutions to this that will automatically do the security updates for you. All you have to do is just have one of those.

Peter Basch – MedStar Health – Medical Director
No, what I'm saying is how does someone verify that? How does ONC or whoever the proxy is verify that hundreds, I mean, thousands of offices, hundreds of different software?

Deven McGraw - Center for Democracy & Technology – Director
They don't.

Peter Basch – MedStar Health – Medical Director
Verifying that everyone is doing that across the country.

Deven McGraw - Center for Democracy & Technology – Director
They don't, and they can't.

Peter Basch – MedStar Health – Medical Director
Yes, right.

Deven McGraw - Center for Democracy & Technology – Director
They don't, and they can't, and that's true for a lot of the meaningful use criteria. You are reporting that you're doing what you're supposed to be doing to CMS in the same way that you attest that you've provided the service that you're billing Medicare for. Part of what keeps people honest, other than generally that a lot of people are honest, in general, is this notion that you could be audited, and there are consequences associated with lying to Medicare, essentially.

Paul Egerman – eScription – CEO
Right. Although there are also technical solutions….

Deven McGraw - Center for Democracy & Technology – Director
Yes. No, I get it. I mean, I get it. But there's only so much we can do here.

Paul Egerman – eScription – CEO
…and you could have certification criteria that requires….

Deven McGraw - Center for Democracy & Technology – Director
That's right.

Justine Handelman –BCBS – Executive Director Legislative & Regulatory Policy
Yes. That's what I was going to say. This is Justine. Isn't a lot of this addressed in the certification rule in the standards section…?

Paul Egerman – eScription – CEO
But getting back to this security update issue, I guess I'm suggesting that our recommendation should include clarification, and it should have the thing that Deven said that I think it should also say that security updates should include security updates from vendors and be very specific that these need to be applied within, say, 90 days of when they're available from vendors.

Deven McGraw - Center for Democracy & Technology – Director
Hold off on that. What if it's expensive? What if it's not free?

Judy Faulkner – Epic Systems – Founder
And also, the other thing is that I don't think you can apply. It depends on what your organization is, but if you're a large organization with 12 hospitals, and the security update is in the next few weeks, it is embedded in code that is going to take months of preparation and testing and alerting people and retraining. You can't say that in 90 days it will be in.

M
Right. That applies really to everybody. Right.

Deven McGraw - Center for Democracy & Technology – Director
I mean, I think we'd have to be certainly careful about how that was worded, and I'm not sure that I would agree that sort of a hard requirement to implement every security update that's in the technology you purchase makes sense. Again, as Justine just mentioned, we've got some security criteria that have to be in the systems to be certified. Arguably, if something comes, you know, if there's a security update that's offered by the vendor, in particular when it's not free or if it is free, but nevertheless, it has some functionality that the provider perceives to make it more difficult to get their work done, I'm not sure it makes sense for us to require automatically that it be adopted.

M
Not only that, but there are situations that occur fairly often, at least in a large hospital environment, where you might have three or four pieces of software, which you're using together. Because one doesn't support a particular technology, you can't implement an update to the other one. By example, would just say that there's a technology that one application only supports a certain version of Windows, and the other one – therefore, you can't upgrade the other ones until that piece of software will support a newer version of Windows because they won't all work together then.

Paul Egerman – eScription – CEO

Yes. I'm aware of these issues, and maybe, since we're going to have another meeting, is we could start to draft some language around this issue.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
I also just want to make an observation, though, is that this aspect of the security environment is about to change because what we're talking about is sort of like this new world where there's a lot more patient access to these records or trying to get the patient portals or something that institutions will be developing. And we're trying to talk a lot more about interoperability, about sending and receiving data. As these systems become more and more open, dealing with these kinds of security issues, the exact kind of issue that was just talked about in terms of how Windows work, is going to be more and more important for healthcare institutions to try to figure out what to do with.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

W
And wouldn't it make sense too for part of the provider education component that they be educated on making sure their contracts have appropriate upgrades, as needed by the vendors, written into their contracts?

Peter Basch – MedStar Health – Medical Director
Yes. This is Peter. Just to clarify that, typically people that have ongoing subscriptions or contracts with vendors include in their support agreements upgrades. The issue is less, in my view, the cost of an upgrade, but sometimes, and this is an issue we're facing at our health system now that the upgrade is free or the upgrade potential might even be in the base product, but hasn't been turned on. But the capabilities to operationalize it require huge changes to the database server or the other environment. And, in our case, the upgrade is free, but the server upgrades to have the horsepower to make it work well and not degrade performance of a system for 2,000 concurrent users is going to be $0.5 million. And it's something we have to do.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Peter Basch – MedStar Health – Medical Director
But it's not something that we could say, if we got 90 days notice that we could do something like that.

Deven McGraw - Center for Democracy & Technology – Director
Right.

M
Typically you base upon budget year, so if you missed the budget year, and all of a sudden there's a need to upgrade, you might be waiting for 12 months or more.

Peter Basch – MedStar Health – Medical Director
Correct. And that's from a system that wants to keep up to date and do all these. It's not from one that wants to drag their feet.

Deven McGraw - Center for Democracy & Technology – Director
Right. Let's see if we can't, in the interim, before our next call, find some language that tries to, forgive the pun, split the baby here, acknowledging the importance of incorporating updates, but with some way to phrase it so that we're not sort of forcing providers to do every single update….

W
Well, there's another really interesting issue that's going through my head, and that is, what this is doing is forcing providers to get maintenance from their vendors.

M
That's right.

Judy Faulkner – Epic Systems – Founder
And I don't know the statistics on what percent don't do that. I know, for us, all of our customers do that, but I don't know if that's true with the one and two doctor clinics. What keeps going through my head, as I listen to all this, is that I've heard people say that the rules and regulations and even just the competitive environment is going to end the one and two doctor clinics. I wonder whether we are continuing on that track, and whether in fact it's the right thing because that's what the patients need. That's what the country wants, or is it….

Deven McGraw - Center for Democracy & Technology – Director
Judy, please. We're not going to talk about the rightness or the wrongness of that. We know they're out there, and we need to make sure that the rules accommodate them, and can we please just leave it at that.

M
But just to go back to what Judy said, I mean, it's a good point, but I can say that virtually all the small practices, even solos, have maintenance.

Judy Faulkner – Epic Systems – Founder
Okay.

M
Because of these reasons. Now once they go on electronic health records, it's a new world. They all do.

Peter Basch – MedStar Health – Medical Director
This is Peter. I would concur with that as well, and forgetting about the philosophic argument about small practices and virtual small practice and virtual groups and so forth. I think that it is reasonable to expect that a small practice that bought a "EHR system" and I'll use quotes because the documentation system years ago and isn't paying support because they feel all they're doing is typing notes in the system is not what we're talking about. And I think that actually it's a reasonable requirement for people entering the current world of an EHR environment, regardless of size of the practice, to have a support and upgrade agreement with somebody, whether it's their vendor or somebody else who's acting on behalf of the vendor. Otherwise it's not just for privacy and security reasons, but you're facing unsafe environments because there are quarterly updates for new medications for the medication database, drug/drug, drug to allergy interactions that don't get upgraded, new codes for new procedures.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Peter Basch – MedStar Health – Medical Director
So that environment that you're talking about, Judy, if it exists, it needs to stop anyway.

Judy Faulkner – Epic Systems – Founder
I'm okay with that.

M
Yes, it really … this situation, even the small. I think what this is going to do is it's going to call out these components of maintenance. I mean, it's going to become part of maintenance and support, as this is pushed through.

Peter Basch – MedStar Health – Medical Director
Right.

Deven McGraw - Center for Democracy & Technology – Director
These are great points. Thank you all. Does anybody else have anything else to add before we go to the sort of second phase of this, which is talking about whether we would argue for some of the rejected criteria to be put back on the table, or even new criteria that weren't specifically mentioned in the proposed rule? This is with respect to what we would say about the security update.

M
Deven, one just last thing, are we all in agreement that the risk assessment and action upon that and the updates are separate issues? Are we going to call that out and make sure that's clear?

Deven McGraw - Center for Democracy & Technology – Director
I mean, I thought that's what I heard. If folks disagree with that, speak now, please.

M
Okay. That's fine.

Deven McGraw - Center for Democracy & Technology – Director
Okay. Great. Keeping in mind, I just want to pause for a second. We have a workgroup that is fairly large in its membership, and I wanted it that way because I wanted to make sure we had a broad range of stakeholder groups. But that may mean for some of you that maybe there's a point that occurs to you after the fact, or that you're not able to get in.

Please feel free to communicate with me by e-mail in the interim. It's the reason why I like to sort of put this stuff up as early as possible, so we have at least an interim meeting to make some midcourse corrections if we need to. Just pointing that out if you think of something after the fact. Send it to me by e-mail, and we'll get it under consideration, whether it's an e-mail to the whole group. There's been some back and forth that way, or just to me, whatever if your preference. And I will never ever consider anything settled per se just because there's been an e-mail conversation because I won't assume that everybody has had a chance to weigh in necessarily.

All right. Moving on to this sort of second phase of meaningful use, which is dealing with what I called rejected or new meaningful use criteria. This goes to the policy committee recommendation regarding HIPAA compliance not being accepted in the proposed rule for meaningful use, the fact that the data transparency for patients was identified by a goal, but not really addressed, and I've got here a suggestion that we might think about how to address it in stage two with more specific criteria, in part because we were told, at least at the policy committee meeting, that anything that wasn't really dealt with in some way, shape, or form in the proposed rule, that it would be very difficult to get it into the final rule for stage one, based in part on sort of administrative law concepts about whether you can add something totally new after a proposed rule has come out. But also, I think, just the shear likelihood of adding to the volume of meaningful use criterion stage one beyond the sort of core pieces that are already there. But I'm putting that on the table again because it got raised in the last call.

Then the third thing that I have here is how to better connect sort of these security assessments and the implementation updates more toward actual use of the functionality that's going to have to be in a certified EHR. Again, there isn't really a clear connection, and if we wanted to make one, I think there's a secondary consideration that we have to think about, which is whether you would make that part of meaningful use, which sets a higher bar for the meaningful users, versus urging ONC or really actually it's OCR, the Office of Civil Rights, to take a look at the security rule for an upgrade, given that we're moving more aggressively into electronic health records than was the case with HIPAA originally. Let me lay that out there and get some feedback.

Peter Basch – MedStar Health – Medical Director
This is on any of the…?

Deven McGraw - Center for Democracy & Technology – Director
Yes, on any of them. Yes.

Peter Basch – MedStar Health – Medical Director
So on the first one, on the….

Deven McGraw - Center for Democracy & Technology – Director
Yes, maybe we start with the HIPAA … you know, whether HIPAA compliance ought to be back in.

Peter Basch – MedStar Health – Medical Director
Yes. Okay, so a couple of what may be dumb questions here, but it never stopped me before.

Deven McGraw - Center for Democracy & Technology – Director
There are none. There are no dumb questions here.

Peter Basch – MedStar Health – Medical Director
Believe me, I know there are some, and I often ask them, but anyway, here we go. I know that one of the issues right now is that many people think that formal HIPAA investigations aren't occurring enough, and if I ask the question, how many HIPAA investigations are ongoing now would be kind of part A question. But under a revised scenario of the Feds taking this more seriously, do we envision lots of HIPAA investigations going on?

The reason I ask this is that one of the things I hear more from hospitals, less from doctors, particularly larger hospitals, there are certainly always complaints and issues going on. I know you address that, as we're talking beyond the complaint stage.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Peter Basch – MedStar Health – Medical Director
But what does it take to move something to a formal investigation? And under a heightened sense of we need to do more for HIPAA, could we see thousands of HIPAA investigations going on, perhaps many per

hospital? The part C of my question is, if that was the case, and … sub one and sub two, how long do they take to go through an investigation now, and if we ramped up the volume exponentially, are we talking about months or years?

The reason that I'm looking at that is I actually like the principle and was in support of it initially until someone raised the issue to me of could there be a sufficient number of, in essence, nuisance investigations or an angry patient that keep raising an issue that may or may not be legitimate, but it's investigated? That because meaningful use is right now all or none, that they could put meaningful use dollars permanently on hold, which would be forever for no good reason?

Deven McGraw - Center for Democracy & Technology – Director
Yes.
Peter Basch – MedStar Health – Medical Director
And I could be completely wrong because I like the notion that if you are violating HIPAA, your meaningful use dollars should be held in advance, but I just don't know if it's possible to operationalize that without penalizing primarily hospitals.

Deven McGraw - Center for Democracy & Technology – Director
Right. That's the reason why, I mean I don't know the answer to sort of how many complaints get to sort of formal investigation stage and whether there's some sort of specific trigger, for example, in the enforcement rule piece that we can latch onto. Another potential option is to just direct this at those who are facing penalties, so therefore you've definitely got somebody for whom the Office of Civil Rights has ratcheted up the level of investigation all the way to, you know, they're basically ready to hit you with a set of penalties, and so you're definitely well past just the complaint stage at that point and into some more serious territory.

Peter Basch – MedStar Health – Medical Director
Right, and then the meaningful use dollars would be held until the penalty is paid, or you would be ineligible if you received a penalty?

Deven McGraw - Center for Democracy & Technology – Director
Yes. No, I think the latter. I don't think we have the right to statutorily do a sort of permanent bar.

W
I think we have Sue McAndrew on the phone. Sue, is there anything here you can offer?

Sue McAndrew – OCR – Deputy Director
A couple of points: One, in answer to the question what is going on at any given time, we have anywhere between, it hovers around 5,000 open investigations or open complaints at any given time.

Peter Basch – MedStar Health – Medical Director
So these are complaints that are being formally investigated?

Deven McGraw - Center for Democracy & Technology – Director
Are they formally or informally investigated?

Sue McAndrew – OCR – Deputy Director
Well, that's the thing. We don't have, and we had not ever used the term formal investigation. That was a term – the only time, well, that term surfaced only with respect to the HITECH Act with regards to willful neglect cases invented this term and said that where there is evidence of willful neglect, the Secretary

must formally investigate the case. But until that time, there really wasn't any concept of formal or informal investigation.

What we do have is informal resolution, which is resolving the case through negotiated, corrective action with the covered entity. And that includes everything up to and including the resolution agreements that we have issued with respect to CBS and the Providence Hospital, which do include payment of settlement amounts. But these are all encompassed within an informal resolution. But, at that point, the investigation itself is over.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Sue, this is Paul Tang. Is there a state between convicted and sentencing … to make the analogy between….

Sue McAndrew – OCR – Deputy Director
That's not my world.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
In a sense, so either they've acknowledged or you've proven that there's been a violation, and the sensing is generally you're working with them to resolve it. So the difference between the June 16th recommendation and the July 16th recommendation was making it clearer that it was not just under investigation or, to address Peter's concern, a complaint has been filed. But we wanted to catch … being conviction, yes, it's agreed, and how we're going to deal with it. So that was changed.

Sue McAndrew – OCR – Deputy Director
I mean, the closest thing that we would have would be those cases for which we are unable to achieve informal resolution and, therefore, we would be issuing at that point a notice of determination that we will be imposing a CMP.

Joyce DuBow – AARP Public Policy Institute – Associate Director
I also want to know whether there's a distinction between paying a penalty and the curing of the violation.

Deven McGraw - Center for Democracy & Technology – Director
I think that's what Sue is speaking to, Joyce. In other words, the informal resolution period, Sue, please correct me if I'm wrong, is the period in which you're supposed to correct what you did wrong. And so, if they're not right….

Sue McAndrew – OCR – Deputy Director
Let me say, there is always corrective action.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Sue McAndrew – OCR – Deputy Director
You must always cure – if the allegation shows an indication or indicates noncompliance, you must cure that through corrective action that's satisfactory to the Secretary. In some cases, in addition to curing that, the Secretary may, depending on the seriousness of the action, impose or take it to a resolution agreement, in which case we would be seeking a settlement amount, but that still is not a CMP.

Joyce DuBow – AARP Public Policy Institute – Associate Director

But what I'm trying to find is a point beyond which, if we're trying to identify a specific point where we are confident that somebody has corrected the violation, I want to know whether the payment of the penalty, does that confirm that the violation is cured? In other words, a specific point in time when that violation is recognized as cured by the Department.

Sue McAndrew –OCR – Deputy Director
By and large, it is recognized as cured by the Department when we issue the closure letter for the investigation.

Joyce DuBow – AARP Public Policy Institute – Associate Director
So that's the point that we need to identify.

Deven McGraw - Center for Democracy & Technology – Director
Well, I think there are a couple of points, Joyce. One being sort of when the bar is lifted, and you can get your meaningful use dollars, which it sounds like we might be able to trigger it to this notice of closure.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Right.

Deven McGraw - Center for Democracy & Technology – Director
But I think we're also looking for the trigger for the bar in the first place, and so….

Joyce DuBow – AARP Public Policy Institute – Associate Director
Well, I guess I'm suggesting that if there is a pending violation, then that would suggest that they shouldn't be eligible.

Paul Egerman – eScription – CEO
This is Paul Egerman. I guess I have a couple of comments about this. One is, the concept of suspending the payments while there's an investigation going on just strikes me as a real problem from the standpoint of due process. Just because you're being investigated doesn't necessarily mean you're going to be found guilty of anything. That's one observation. The second observation I have is it seems like CMS already said no to us on this thing. And as I listen to some of these discussions, it seems like they have an entire process already in place, and they have a lot of remedies, I guess, that the law already involves. I'm just wondering if we're doing anything valuable here because … say no again.

Deven McGraw - Center for Democracy & Technology – Director
You may not remember this particular part of the policy committee, but I actually asked Tony Trenkle from CMS about this, and their major concern in taking it out was the sort of lack of a clear trigger for when people would essentially be what I'll just refer to as on suspension and not have their meaningful use payments. Not that they had any fundamental disagreement with where we were headed here, but they just didn't want to do it as a complaint stage. They weren't sure that they had a clear trigger, and in fact Tony expressly invited us if we had some more specific language to offer it. So I actually think it is a value to have the conversation.

Paul Egerman – eScription – CEO
Okay. I guess I did miss that, and so if it helps them, and it's a solving of a problem for them, if it helps them with enforcement, then certainly it's a good idea.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Can I suggest that there's another way to look at this, and I think I'd brought this up before is that if you are certifying that you have met these criteria, and it later comes to light that you have not met the criteria, and your certification is in fact false, the bigger issue in my mind is if an organization has been provided with or given large amounts of money associated with meaningful use and later found to have a defective certification, not just these certifications, but other ones. Is somebody going to come back and ask for their money back? Is that sufficient leverage to cause people to not want to misrepresent certifications?

Terri Shaw – Children's Partnership – Deputy Director
This is Terri Shaw. To that point, I agree with that concept, but as far as I can tell, there is no requirement that you certify HIPAA compliance beyond the security provisions as part of this standard.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Terri Shaw – Children's Partnership – Deputy Director
So while I agree that that would be a great concept, there's no fundamental certification of that in the first place that would allow that to occur. I personally am for finding ways to make the rule clarify that using technology to protect information goes beyond just security. It also includes privacy. This is potentially one way to get that. I agree with you. There could just be a certification that you're in compliance with the rules, so there may be other ways to achieve it. But I do agree that finding some way to include privacy as part of that standard would be preferred. On this particular solution, just to clarify what it is that we're talking about, so I understand, two questions.

Deven McGraw - Center for Democracy & Technology – Director
Sure.

Terri Shaw – Children's Partnership – Deputy Director
One is, are we talking about suspending the payment during the times that this investigation is happening, however we define it, and then not just turning the payments back on, but giving back whatever, you know, paying out any money that would have been paid during that time? Are we talking about full restitution of all payments owed, or are we talking about just picking them up again from the point at which things are cleared? That's one question. Then the second question is, at the risk of opening up a huge can of worms, as I understand it, ARRA now gives attorneys general the ability to enforce HIPAA as well.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Terri Shaw – Children's Partnership – Deputy Director
And so, does formal investigation also include those investigations, as well as OCR's?

Deven McGraw - Center for Democracy & Technology – Director
All very good questions. I think what we intended with respect to the … that I don't think we have the authority under the statute to, I mean, if you're otherwise eligible for a meaningful use payment, and what's keeping you from getting it is that you've got a HIPAA compliance issue, for example, that you haven't resolved, again assuming that there were to be some criteria that required you to either certify to that. Once you've sort of, I mean, again, depending on the series of triggers, you'd have to be eligible for your full payment. I don't think there's anything in the statute that gives authority for you to somehow get less or not get the full amount of what you otherwise would be eligible for under the criteria. But we'd probably have to be clear about that since these payments are staged.

So if you otherwise would have been eligible in stage one for the first year of payment, and what was barring you, I mean, this is certainly how I think we envisioned it was that you had a HIPAA problem that went beyond the complaint stage. Once that got resolved, so I like the concept of a closure letter, CMS would then have to pay you the money.

W
But isn't there some penalty implied by some kind of lapse in time because the payments vary by when you qualify?

Deven McGraw - Center for Democracy & Technology – Director
Yes, but I guess I don't see, I mean, and we can certainly check with CMS on this, but I don't see how, if you were eligible for a stage one payment, and this was your bar that you would, I mean, I think we'd have to be clear that the intent was not that you would miss it entirely. I don't see anything in the statute that would prevent—

W
I'm simply suggesting that the eligible would occur at the time you are fully eligible. And I you fail to comply within the timeframe of stage one, for example, you would be bumped down.

Deven McGraw - Center for Democracy & Technology – Director
Right.

W
It feels to me as though that's a deterrent.

Deven McGraw - Center for Democracy & Technology – Director
I see what you're saying.

W
I think that this is an opportunity to insure HIPAA compliance, and we need to find the first trigger that CMS was asking the policy committee to identify because we seem to have identified a closing trigger, which is the closure letter. So I think what we need some guidance on is finding the first trigger.

Deven McGraw - Center for Democracy & Technology – Director
Right.

W
Because I think it's fair to say that somebody should not be determined to be guilty before there is some request for a cure.

Deven McGraw - Center for Democracy & Technology – Director
Some process, right.

W
And so what we need to know is what is that official request. When does that occur? How is it conveyed by OCR, for example, that you must cure X? What do you do?

Peter Basch – MedStar Health – Medical Director

Also, this is Peter, the timeliness of that because, indeed, if this is framed, and you're correct, at least by my read that meaningful use is all or none at any given measure year that regardless of attestation. If there's a HIPAA privacy investigation going on that you would not qualify otherwise for that measure year unless you miss a year. If an investigation takes longer than X period of time, that could be problematic as well. I can't remember who made this comment before on the call that there about 5,000 investigations going on now.

Deven McGraw - Center for Democracy & Technology – Director
It was Sue McAndrew.

Peter Basch – MedStar Health – Medical Director
Okay. To know whether that is 5,000 directed at 5,000 unique individuals or 3,000 hospitals. Basically, are we saying that almost every hospital has a HIPAA investigation going on now? Are there 1,000 complaints against one doctor who should be behind bars? I'm asking it not facetiously, but just to know what the state of the state is, and with some notion of upping the level of investigations has been called for. Will we be saying, particularly if the process of resolving these is going to take a significant period of time, will we be essentially saying that the way we want to frame this rule will essentially disqualify half or a third or 20% or 80% of hospitals from meaningful use payments just because of the process for investigation? That would be a problem.

Deven McGraw - Center for Democracy & Technology – Director
Well, it would, but we've got to….

Peter Basch – MedStar Health – Medical Director
I mean, if we could assure the equivalent of a speedy trial….

Deven McGraw - Center for Democracy & Technology – Director
Yes. We've got a bigger problem than that if 80% of hospitals have violations that are at the serious level that we're trying….

Peter Basch – MedStar Health – Medical Director
But we're not saying that they're necessarily serious. They're being investigated.

W
But we have to assume that they're not frivolous.

Peter Basch – MedStar Health – Medical Director
Understand.

W
…investigations aren't precipitated frivolously, but I think your point is fair. I just think we have to better understand it.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Sue McAndrew – OCR – Deputy Director
This is Sue McAndrew. I mean, some of them may prove to be frivolous. Some of them may prove to be not a real violation. But even where there are indications of violations, many of these cases do involve issues of failure. A complainant did not get the access that he requested. This may turn out to be a

single case of an individual who did not get access. In other cases, it may be something, it may disclose something that is systematic within the entity. It may be an individual who thought the reception area that the receptionist was speaking too loudly and called out his name too loudly in the reception area.

It could be someone who has a serious – you know, we are now getting breach notifications, and each of those will go into investigation, so it could be some computer disk was stolen, and that has exposed thousands of names potentially to misuse. And so we really have a range, a broad range of issues that come up to us in the form of complaints. And I think the question for you all is what do you see as a sufficiently egregious or serious noncompliance that you are concerned about the meaningful use fund. We had talked just briefly before about whether the notice of determination for initiating a CMP action would be the threshold for that kind of serious violation.

Deven McGraw - Center for Democracy & Technology – Director
CMP is civil monetary penalty, right? In case folks don't know.

Sue McAndrew – OCR – Deputy Director
Yes.

M
But are civil monetary penalties apply – I don't know enough about when they're applied or how they're applied and whether they would be applied equally to a computer that was stolen, and there was a breach, and the same toward a kind of willful negligence.

Paul Uhrig – SureScripts – Chief Privacy Officer, EVP Corporate Development
Right. This is Paul Uhrig. I mean, I think the other issue that Sue's comments bring up to me is, is it appropriate to use the meaningful use rule around healthcare technology to enforce compliance with things that have nothing to do with healthcare technology like a nursing speaking too loud?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
This is Paul Tang. I think the intent of this category, privacy and security, was to be foundational. We've said this was very important to trust, so I think it is part of meaningful use of this technology is that you have to comply with the privacy rule and privacy and security rule. Now we do have the problem of a lot of these cases, can we hold up meaningful use of the entire system throughout the enterprise on some of these individual cases? But I think actually the Recovery Act does give us this tiering of egregiousness. Perhaps one of the thoughts is to look at the highest tier or highest and second highest, whatever we choose, and say that actually clearly is a deliberate misuse of this technology, and that would definitely not be a meaningful way of using this technology to improve health outcomes.

Deven McGraw - Center for Democracy & Technology – Director
Yes. That's a suggestion. I think the other suggestion is maybe – I'm trying to think of, because I don't have my statute in front of me. I'm trying to think of the tiers are specifically directed to the egregiousness of the offense.

Sue McAndrew –OCR – Deputy Director
The HITECH tiers, the highest is uncorrected willful neglect.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Sue McAndrew – OCR – Deputy Director

Below that is corrected willful neglect. Then it's reasonable cause, and then it's not knowing.

Deven McGraw - Center for Democracy & Technology – Director
Thank you, Sue.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
I think, when we get to willful, so that's the top tier and the tier below, we're talking about deliberate. It's been determined, and there's probably an extensive process to determine that. So if we know that it was willful neglect, I don't know that that qualifies an organization to receive, to be deemed a meaningful user of the HIT to improve health outcomes.

Deven McGraw - Center for Democracy & Technology – Director
And protect privacy.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Well, I think protecting privacy is part of meaningful use.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
So I think that's, so that's the … suggestion to put on the table.

M
Could you read the language of the top two tiers again or the most egregious two tiers? Both are willful neglect, but….

Deven McGraw - Center for Democracy & Technology – Director
The top two are both willful neglect. The second to the top is it was willful neglect, but you corrected it.

Sue McAndrew – OCR – Deputy Director
Yes.

Deven McGraw - Center for Democracy & Technology – Director
And then the very top tier, the highest degree of penalty is willful neglect, and you didn't fix it. I mean, that's almost a head in the sand kind of example.

M
I certainly think that gives us some bars to think about. Now how we operationalize those, and I guess what I'd want further clarification on is an example of what willful neglect actually means because certainly there's a layman's interpretation. I think, to all of us it means these are people who probably shouldn't be practicing medicine. My guess is, if we could look at some of kind of a summary of anonymized cases, we might feel differently, or maybe not.

Sue McAndrew – OCR – Deputy Director
There is a definition of willful neglect in the regulations.

Deven McGraw - Center for Democracy & Technology – Director
Yes, which we can circulate to folks.

M
Yes, that would be useful.

Deven McGraw - Center for Democracy & Technology – Director
How about if we do that? We sort of focus again on those top two categories and try to come up with some trigger language that also has some specific definition and uses some of the terms that Sue brought up today with respect to you're getting a determination. There's a civil monetary penalty action, and it's at that highest, at least the top two tiers, if not just the top tier, and then the bar is off when you get your closure letter.

W
That sounds like a good idea.

M
It sounds like a plan.

Deven McGraw - Center for Democracy & Technology – Director
All right.

W
Deven?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

W
I would just say one other thing with regard to how some of these cases – what would constitute closure of some of these cases. For instance, if we do take willful neglect case to a CMP and issue a notice of proposed determination, the entity does have appeal rights.

Deven McGraw - Center for Democracy & Technology – Director
Right.

W
So they can first go through an ALJ proceeding, which will either sustain our actions for the CMP, but we can't enforce the CMP until after the ALJ has ruled. And even after the ALJ has ruled, the entity does have the right to go into court to challenge that determination.

M
Is that an administrative law judge?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

W
Yes, administrative law judge.

M
Thank you.

W
Is there a timeframe within which that process has to occur?

W
There is a timeframe in which the entity has to request the hearing. Then there are some procedural time limited filing, but I think it is generally driven by when the ALJ can docket the particular proceeding. It's not like this whole thing has to be wrapped up within a year.

Deven McGraw - Center for Democracy & Technology – Director
Right. Yes.

W
I was going to ask you the average timeframe.

W
Well, there is no average because we haven't exercised. We haven't had a case go to an ALJ. We haven't exercised the CMP authority.

Deven McGraw - Center for Democracy & Technology – Director
You know, one of the other things that I'll do some checking on offline with Tony Trenkle and/or his staff and folks in the legal counsel office within HHS is whether if in fact those investigations took too much time, whether folks could, you know, whether they sort of run out of time to get their money, which is a point that others brought up on the call. I mean, I think I was just assuming that once the investigation closed, as long as you were otherwise eligible during the payment year, you could still get a payment, but now that's not 100% clear to me.

M
Right, and I think the other part of that question, Deven, is that, as I'm thinking about how the statute is written, and in terms of no incentive payments will be made beyond X year, that it may indeed be that once you move beyond the payment period for a measure year that it may just not be able to be paid out.

Deven McGraw - Center for Democracy & Technology – Director
Right. I'll definitely check on that because I know that's pertinent to us being able to make a decision here.

M
Okay.

Deven McGraw - Center for Democracy & Technology – Director
Good discussion. More to come in the next call. There were two other things, again, the mention of data transparency to patients and consumers. The fact that it was mentioned on the matrix, but even the meaningful use group hadn't really put forward any specific sort of objectives or measures in part because we had HIPAA compliance as an objective and measure, and that there are transparency requirements in HIPAA already.

The other thing that I noted here is that I'm not sure that we necessarily intended to single out data transparency as necessarily more important than other privacy issues. It's just that we definitely had identified it as a priority, but I don't – and Paul Tang and others on meaningful use workgroup who also serve on this workgroup can tell me if they think I'm wrong. But it just didn't get that kind of focus. So essentially what I was putting out was that we sort of look at what we might think about to recommend for the stage two requirements on privacy and security, and consider data transparency with a host of other sort of priorities that we might put forth at that particular time rather than trying to think now about some criteria here for data transparency absent really much discussion at all in the proposed rule, which doesn't give us much of a chance of moving it forward in the final.

And then the last piece of this is whether we want to create some sort of linkage in meaningful use or through recommendations to update the HIPAA security rule to tie more closely what providers do on security with the sort of functionalities that are now required to be in the technology. Does anybody have a problem with thinking about data transparency in stage two? Okay. Great. And it wouldn't be just that, but we sort of think about what priorities we might pull out for a second stage of measures.

Terri Shaw – Children's Partnership – Deputy Director
Deven, this is Terri Shaw.

Deven McGraw - Center for Democracy & Technology – Director
Hello, Terri.

Terri Shaw – Children's Partnership – Deputy Director
On that note, transparency seems like a good one to investigate to me. The other thing that I kind of referenced earlier that I think is lacking is that the objective here on this particular – what's already in the proposal is to protect information through implementation of appropriate technical capabilities. But then it only refers to security. Are there other ways that we could get at now required or at least indicated technical capabilities that are about privacy, and we can cross-link to at least those earlier rather than later since we know that theoretically people are already going to have to be doing those. For example, the IFR, as I understand it, includes some specifications around accounting for disclosures.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Terri Shaw – Children's Partnership – Deputy Director
Is there some way to link to that through attestation or otherwise, but to build an acknowledgement that you not only have to have that capability in your software, in your EHR, but you actually have to be using it to accomplish the HIPAA requirements, for example.

Deven McGraw - Center for Democracy & Technology – Director
Right. Right, which….

Terri Shaw – Children's Partnership – Deputy Director
So is there something like that we could build on?

Deven McGraw - Center for Democracy & Technology – Director
Right. Are you talking – are you sort of laying it on the table as a potential stage two conversation?

Terri Shaw – Children's Partnership – Deputy Director
I'm assuming that that's probably, as a practical matter, what will have to happen. But I defer to others who are much more enmeshed in this.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I mean, I think, in part, not only is it practical, but we also have the issue of, you know, we've got the standard or the sort f functionality for the technology, but the Civil Rights Office still has six months to

come up with a regulation about what needs to be included in that. And I think all of that process just pushes out that timeframe even further. There's a set of timing deadlines that are as early as, I think, 2011 for new technology adopters, but the Secretary has some authority to extend that. At any rate, I think that's a good suggestion to essentially put on the potential priority list, especially given that it's a new requirement in ARRA, but I just don't think we can get it done for stage one.

W

But can we express some interest now in seeing that it does get addressed, that we're concerned about it?

Deven McGraw - Center for Democracy & Technology – Director

Yes, we can certainly, at a minimum, I think, say that it's something. I mean, focusing on what would be needed for accounting of disclosures was also on our sort of tentative work plan, again given that it's a requirement. So I don't think it's at all out of bounds to say that we're going to be looking at that and may have something specific to say with respect to stage two.

Terri Shaw – Children's Partnership – Deputy Director

This is Terri again. I also think that we may not be able to do this in time for meeting this comment period, but I assume that as further development through the committee and otherwise happens on things like additional certification requirements over time to include, for example, capabilities, technical capabilities to support consumer preference choices: consent, authorization, what have you, which I know is a whole other discussion that we'll get to at another time on the consent issue. But just to acknowledge that as the technology develops and the standards develop and the criteria develop, those should be reflected as part of these meaningful use requirements over time.

Deven McGraw - Center for Democracy & Technology – Director

I've actually got, and I don't know how close we're going to get to being able to touch on it today, but I've actually got sort of technological functionality to help providers comply with patient choice requirements or policies that are already in affect on deck to talk about a potential early stage because they exist in the law today, and this is something that, again, we'll get to it, I think, in just a second or minute or so. I mean, this is something that I was actually told during the policy committee meeting that they weren't provided a standard for by the standards committee, but I'm not necessarily sure that's true. Is Dixie on the phone, Dixie Baker? Okay. We may not be able to get into this in any more detail, but when we get to that….

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Deven?

Deven McGraw - Center for Democracy & Technology – Director

Yes?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. I just wanted to note that there are, on the ONC Web site, presentations by Dixie Baker about recommendations made from the HIT Standards Committee and discussed with the HIT Policy Committee relating specifically to access control.

Deven McGraw - Center for Democracy & Technology – Director

And access control is what enables you to essentially manage – to use the technology to help manage patient preferences, patient consent.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes, so this was presented, and I can send the links to everyone, so they can go see that this was in fact discussed.

W
That would be great.

Deven McGraw - Center for Democracy & Technology – Director
Okay. So we've actually got that teed up on the agenda, so if we can just hold off for a minute so we can close out this discussion about linking sort of, again, the overall point being that there are these sort of technical functionalities that are required to be in certified EHR technology that are related to security, and yet we don't necessarily have a requirement from a policy standpoint to use them, either as part of meaningful use or as something that you are sort of required to address in the HIPAA security rule. They're all addressable, meaning that you should think about whether you want to put them in place. Sue McAndrew, you can correct me if I'm mischaracterizing this, but it's certainly not a requirement, for example, to use encryption when you're transporting data.

There are lots of incentives to do so, especially now with the breach rule and the Safe Harbor, but it's not a requirement, per se. So I was trying to think of a way to connect what is required under meaningful use under security with those functionalities, and I think initially I thought, well, why not think about meaningful use meaning now that you have these functionalities, you have to use them, and that should be part of meaningful use. But I'm concerned that just imposing those requirements on meaningful users versus approaching stronger security requirements through an update to the security rule, which would take longer, but which would avoid the sort of disincentive to adopt the technology that might take place if we sort of load too much into that meaningful us bucket.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. I'm wondering, though, the certification criteria at least could fill out some of these requirements for the certification process, so at least the vendors are thinking about making sure those capabilities are in place.

Deven McGraw - Center for Democracy & Technology – Director
Absolutely. I mean, unless I'm missing something, the fact that those capabilities have to be there in order for the EHR technology, either as a system or as a module to get certified, I mean, it'll be there, and it has to be functional. But do you actually use it to protect data? Maybe some of them are kind of self-affecting, but certainly not all of them are, encryption being one where you usually have to make sure it's at least turned on.

I'm going to propose something, which is that we think about that sort of question that I've laid on the table in the context of taking a look, of moving to a discussion on the standards in the interim final rule and what we might want to say about these standards and picking up that discussion as part of that thread. Again, what you've got in your materials, they're moving on to talking about the standards that are required for EHR technology to be certified. You have the table replicated in your materials. It includes encryption, audit log, the use of a secure hashing algorithm to verify that the information hasn't been altered, cross-enterprise authentication, and then some functionalities with respect to complying with the accounting for disclosure rule.

I put down here sort of issues to discuss, and the top one is really this notion of the missing standard here or missing certification criteria appears to be that there wasn't one for access control. The systems are not going to be required to have some sort of functionality related to access control that can help, which helps entities manage the patient consent requirements that the have to comply with an existing law or because their organization has a policy that requires it.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. I wanted to see. Maybe someone can help clarify how that table from the IFR relates to the table one in the IFR, which would be page 28 of the federal register. It has a huge section at the bottom that talks about all of the certification capabilities, and it specifically speaks to access, the control of access, and the recording of disclosures, etc. It's much more explicit than that table, so I think it would be very good to figure out why the table doesn't reflect what is a requirement under certification.

Paul Egerman – eScription – CEO
Yes. This is Paul Egerman. I could do my best to respond to that. I think the table that's in the minutes is intended to summarize the standards that are adopted for privacy and security. But just adopting a standard doesn't necessarily by itself do anything. You have to have the certification criteria, and so the table that you reference, which is not in front of me, is probably a list of certification criteria. And the certification criteria around a standard, but it also can be a certification requirement around what I would call a technical requirement, which does not necessarily have a standard. You could have a certification criteria, as an example, that says all passwords have to have at least six characters. I'm just using that at random. I'm not trying to advocate for that, but that would be certification criteria around a technical requirement that doesn't involve a standard.

Deven McGraw - Center for Democracy & Technology – Director
Okay, but let me just clarify something here. Is it or is it not the case that right now for a system to be certified, it does not necessarily have to have an access control standard in it. It did not look to me like there was a standard for access control, i.e. I often refer to it as consent management because I find the term access control for some reason to be misleading, or I just don't understand how that's linked to managing consent. Therefore, I end up calling it consent management. But at any rate, it doesn't look to me like a system has to have those functionalities in place in order to be certified, but please correct me if I'm wrong.

Paul Egerman – eScription – CEO
As far as I can tell, there's no standard for it, but I'm not sure I know the answer to whether or not it has to have it, in looking at the certification criteria. My point is you can put in functional requirements to have it without specifying a standard.

Deven McGraw - Center for Democracy & Technology – Director
Right. That is right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. The reason that it's confusing is the set of standards in the material that was sent out are not always specified to specific security standards. They are sometimes describing standards from a functional point of view. So you would think that if a requirement to certify that the system, and I'll quote it, "verify that a person or entity seeking access to electronic information across the network is the one that is claimed and authorized to access such information." So you would think that that would also be reflected in the table.

Paul Egerman – eScription – CEO
Well, this is Paul Egerman, it doesn't have to be because that's a good example of certification criteria around a technical or functional requirement for which there is no standard. In other words, they're

saying to the software vendors, you just have to meet this criteria, and you have multiple ways of meeting it.

Deven McGraw - Center for Democracy & Technology – Director
Right, but I don't want to, I mean, maybe … I guess it's possible that I pulled out the wrong table. I don't want to get into a discussion of which table is the more authoritative one with respect to what has to be in the systems. What's more important for this discussion is do you have to have some kind of access control functionality, even if it's not a specific standard per se, in order to be certified. Kathleen?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes. I think we should ask that they make it very clear that if there is a certification criteria for access control, would that be reflected as a functional standard in this table.

Deven McGraw - Center for Democracy & Technology – Director
Okay.

Terri Shaw – Children's Partnership – Deputy Director
This is Terri Shaw. Just to be clear, when we say access control though, we mean both that the person who is trying to access it is in fact who they are supposed to be.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Right.

Terri Shaw – Children's Partnership – Deputy Director
That's one, so identity, which does seem to be reflected in the table that I'm looking at, at least. But then the second part is, and that they are authorized for this particular transaction, that this particular transaction is authorized to occur and to this person. So it's not just that it's the right – that the person has a right generally, that the person is who they say they are, but also that they are properly able in this case to access this information, or looking at it from the other way that the entity that holds the information is authorized to disclose it to that person.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I will send out the certification table, and it speaks to both the access control internal and for across the network. But in addition, access control often means in addition to just actually getting the information, to some kind of permissions or authorizations about how that information is used. For example, you could have a read only access, or you could have an access that allowed you to, in addition, modify the data or to disclose it further.

Deven McGraw - Center for Democracy & Technology – Director
We will definitely have to get some clarification on this because I was under the impression that in fact access control criteria, whether in the form of a specific technical standard or just a requirement for a technical functionally was not in fact in this rule, and that the reason for that was that, I mean, I actually asked this question specifically at the policy committee and thought that I was told, well, we didn't get a policy on that from … we didn't get any recommendation from the standards committee on that, so we didn't have anything to either adopt or not adopt and work with for this interim final rule. And so, I mean, it could be that I just am misunderstanding what's going on here, and we'll certainly clarify it for our next conversation because if in fact there are standards or functionalities in systems that do the access control piece of it that's helpful to adjudicating whether somebody has the right to access information with patient consent, you know, managing patient consent being part of that, then I think that's helpful for us to know.

Terri Shaw – Children's Partnership – Deputy Director
This is Terri again. I agree, it would be great to get that information, and not least of which is because it has ramifications for how health information exchange networks are built and managed and what kinds of services are provided over them. I know there are questions going on at the state level about whether we need to have some sort of central consent management process, and I think the assumption there is because there either won't be a consent management process available in each resident EHR, or it won't be good enough. And so knowing how strong the EHR capabilities are then would help to influence what we do on the HIE side.

Paul Egerman – eScription – CEO
It makes sense. This is Paul Egerman. I agree with your summary of what you need to do, Deven, in terms of doing the review. I actually have one issue that's somewhat related, which is in the IFR, although I didn't go through it in detail. I didn't see any place where it talked about segmentation of the record. To do some of the things that we've talked about like limiting access to sections like behavioral health or reproductive health, you need to have segmentation. And I kind of think one of our recommendations on the IFR should be that there should be something that alerts the vendors that in stage two, segmentation of the record will probably be a requirement. The reason for that is it's a lot of technical work, and we need to get the vendors started on this. This is something that we want to have happen.

Judy Faulkner – Epic Systems – Founder
I think that's a really good topic to bring up. It's a critical topic because I'm not sure what segmentation of the record would really mean. The example that is given sometimes is if I had an abortion 20 years ago, can that be suppressed? I think we can suppress certain things, but my worry is when Gayle Harrell in the meeting talks about trust, I'm afraid that we will not be able to get trust because we can't get rid of everything.

What I mean by that is, even if you segment of the record, there is the appointment information that's stored. You've got the visit to the primary care physician, maybe a visit to a gynecologist, maybe visit to social workers who have notes stored from each. You have the information in the lab system about the lab orders and whatever notes were there. You've got the lab results that are coming back that have not been segmented. You've got the procedure, the room, the physician, the equipment, the case logs, the notes from that. You might have the maternal fetal drug that's given to prevent future pregnancy problems. You've got phone calls if there's follow up. You've got potential followup complications and treatments. You've got medications. You've got financial transactions that go, and my big worry is that we will have – a couple big worries. One, we will have patients who rely on us, and I don't think there's any way we can follow all the threads.

You even have later on the question of, well, what are those three things that they ask you: number of pregnancies, number of births, and something else. Suppose the woman, for a while, said the correct numbers, and later on decided to change that. It could reference the wrong numbers because it doesn't even know how to go look for that in the notes potentially.

W
Yes.

M
It's a separate topic because I agree … points, and I think there are some things that vendors and providers do feel comfortable segmenting. There are others that may be impossible to segment. We want to make sure, as we try and gain more trust of patients, and I think people have been doing that for

a long, long time anyway, that we don't set unrealistic expectations based on the technology, but also based on what's good medical care.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I mean, I think that, at a minimum, I mean, all of this is so closely tied into our conversations about patient preference. But I do think, at a minimum, we can be letting folks know that we're taking that up, and we're going to be looking both at policy, as well as technological functionalities that are going to need to be in place so that we're definitely sending smoke signals, if nothing more specific, that there could be some higher expectations in this regard. But I do think it's a very complicated conversation.

Judy Faulkner – Epic Systems – Founder
It's very complicated and I think, underneath it all, the word trust is so important that if people are trusting this to be hidden, it's going to be almost impossible to really insure that in all the different types of things people might want hidden. Then there's another thing. Even it's things like who is your care team, in many cases, or suppose you want to hide diabetes, and then is your yearly foot exam and eye exam going to be turned down because there's no reason for it. And so I think what will happen is that the insurance companies will have capable people who can spend the time looking for just laughing at the fact that the diagnosis or the meds aren't there, and looking for all those other things, such as the care treatment or the annual appoints for whatever. And they're going to be able to still do the stuff patients are afraid about. But the doctor who only has a limited amount of time will not be able to give that attention to looking through the record for hidden stuff, and will then give poor care. So it is almost like the worst of all things happen.

Deven McGraw - Center for Democracy & Technology – Director
Well, again, let's suspend further conversation on that, again, until we actually have an opportunity to do so, and it's no seven minutes until the end of the call.

Judy Faulkner – Epic Systems – Founder
Sure.

Deven McGraw - Center for Democracy & Technology – Director
On that note, clearly we've got some work to do to prepare for the next call. I did not – I want to ask you all because we're really running out of time here, and we need to open up the lines for public comment as well, to start providing me with your wish lists of sort of what information you think we need to have in order to tackle this patient preference conversation. I think we got a sense of sort of some of the aspects of it, as part of this data segmentation conversation. I know that we will have at least one hearing on this issue. I'm wondering whether it's got to be a series of hearings. But at a minimum, I want to start sketching out a work plan and some timeframes for tackling this, and I need your help.

There's also, just so you know, some work that's been done by ONC, a white paper in particular that looks at the ways that the different health information or exchange organizations have been implementing consent policy, and that should be really helpful, and that's very close to being ready to be distributed to us, or else at least that the sort of high level conclusion is shared with us.

W
Deven, I noted that the National Governors Association just released a report as well coming out of their state, the alliance efforts or whatever it is.

Deven McGraw - Center for Democracy & Technology – Director
The state e-health alliance.

W
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes, if we could get that circulated as well, that would be terrific.

W
I just got that by e-mail. I'll forward it to you, and we'll get it around.

Deven McGraw - Center for Democracy & Technology – Director
Terrific. Well, again, since we're running out of time, I'm suggesting that we sort of start that by inviting you all to e-mail me anything and everything you think is relevant to put on the table, and I'll start sorting that into a work plan.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Deven?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
John Houston. You know, the other thing too is what we had talked about with NCVHS and what types of topics we can help out on.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The idea of the sensitive data types and things like that are something we'd talked about.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I want to leave that also on the table is if it seems like there's more topic than there is capacity, that I think NCVHS can provide some assistance, as necessary, to move this stuff forward.

Deven McGraw - Center for Democracy & Technology – Director
Absolutely, and we want to also be well aware of the work that you guys have already done. All right. With that, I'm afraid we're going to have to – I mean, no. This is the good part of the meeting, of course, opening up to the public, but we'll have to cut our own conversations short so we can have an opportunity to hear from folks not on the workgroup. Judy, do you want to take it away?

Judy Sparrow – Office of the National Coordinator – Executive Director
Sure. Thank you. I'll have the operator open the line for public comment. I know Dr. Peel is in line to make a comment. But while we're waiting for that to happen, I think the next workgroup meeting is February 3rd. Is that right, Deven?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes. Operator, do we have anybody on the line?

Operator
Yes. Our first question is coming from Deborah Peel from Patient Privacy Rights.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. Thank you.

Deborah Peel – Patient Privacy Rights – Founder & Chair
Hello, everybody. First of all, I want to congratulate Paul and the people who brought up the really critical issue of the ability to segment information. Not only is segmentation not in meaningful use and, of course, it needs to be because it's a federal legal requirement for sensitive information, but we have to have these capabilities because, as Paul pointed out, there are many kinds that sensitive information. And John Houston, we specifically disagree that there needs to be categories of sensitive information decided by people other than the patients because patients have privacy preferences that are different, and technology uniquely can allow for them to be expressed. And that's what the AHRQ focus groups found out that people really want to exercise their individual rights to determine what's private.

I think it's really important, Deven, and I totally agree with you about sending smoke signals to the industry. It's really important to tell them that the ability to do this is going to be essential for EHRs going forward. We are very, very aware that many EHRs cannot do this right now, and I'm not enough of a technologist to know whether some of them may never be able to. But the public is never going to stand for eliminating the right to segment information. And so whatever that's going to take, I would urge you to, when you have these hearings, to look at the systems that are already doing this. The NDIIC system enables the segmentation of sensitive behavioral health data, and there are others. The privacy access system allows the segmentation of different information to be presented to clinical researchers. So there are models out there that the nation and the government really need to see.

Frankly, we're kind of tired of industries saying we can't do this. This is very, very familiar from all large industries. If you think of the auto industry, they never would have added seatbelts, airbags, or fuel efficiency if it hadn't been required by Congress. And we really need the innovations to happen.

The other things that I want to point out that are not in meaningful use that are very, very important, really we believe that consent should be part of that, not 2014 or 2015, and in fact, the right to stop the disclosure of PHI for payment and healthcare operations if you pay out of pocket is a HITECH requirement. So that requirement means that there has to be functional consent. And I would point out that in the HIPAA privacy rule itself, it allowed individual doctors or providers to agree to use a consent process for the disclosure of patient records. And so we have to be able to exercise that in every electronic health record systems.

Again, we fully understand industry doesn't want to do this. They never want to do this, but realistically what your job is, is it set the bar and make sure that industry moves in the right direction responsibility over time, but these are existing federal requirements that need to be part of meaningful use and are not. And it's very significant for people who want privacy to at least be able to stop their information from going to health plans, you know, for payment and the rest if they pay out of pocket. The issue is really, when we don't have privacy, how many people will stop getting treatment? And when people stop getting treatment, you can't say that they're getting quality care. So we would just really urge you to set the bar to meet existing federal laws, which really, if you look at them, the right to stop the disclosure of PHI when you pay out of pocket for payment in healthcare operations, that's a consent preference that needs to be put in place as soon as possible.

Americans care the most about this issue in the system, and there isn't another way to have trust, and so I really, really encourage you to stick with your plan on requiring the ability to segment sensitive information and to move up the timelines for meaningful and effective consent. Thank you.

Deven McGraw - Center for Democracy & Technology – Director
Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, Dr. Peel.

Deven McGraw - Center for Democracy & Technology – Director
Thanks, Deb.

M
Judy, just to add in, if anybody else from the public wants to make a comment, simply press star, one on your phone to indicate that you want to make a comment, and the operator will open up the lines one at a time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Nobody else on the line?

Operator
We have no questions at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. Deven, back to you.

Deven McGraw - Center for Democracy & Technology – Director
Great. Then I think we're done. We're a little bit over. Thanks to everyone for really what I think is a great meeting, and we have more materials to come. Get me your suggestions, and have a good day, a good weekend.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you very much.

W
You too. Bye.

W
Bye-bye.